Introduction

The Common Access Card (CAC)

As a Smart Card.

- A credit card-sized device that can contain multiple technologies and personalized information
- Is a portable, protected computer with both processing ability and information

As an ID. The CAC is your new military ID card, providing personal identification along with a diversity of helpful information.

As much more than an ID. The CAC contains a processing computer chip, bar codes, and a magnetic stripe. The CAC:

- Protects personal and national security
- Enables automation of the Army's daily business processes
- Provides stronger security services—to log on to a network, access a web site, and exchange email

Public Key Infrastructure (PKI)

Three DoD PKI certificates containing public and private keys are loaded on your CAC's computer chip to provide digital identification, signature, and encryption.

Getting Started

You can now digitally sign and encrypt email using your CAC/PKI. The following tasks must be accomplished:

Task	Responsibility
Obtaining your CAC	CACs are issued just as previous ID cards—through an ID issuance facility (located on most military installations)
Enabling your desktop for the CAC	Information management specialist
Configuring your email client	Information management specialist
Having your CAC and knowing your PIN	YOU

"REMEMBER YOUR PIN!"

Concepts

Term	Description
Non-Repudiation	Assures that senders cannot deny having sent messages
Encryption	Assures that only your intended recipient(s) can read your message
Digital Signature	Assures that a message originated from the specified sender and remained unaltered enroute
Web/Network Access	Assures greater identity protection and stronger authentication

Operations

Until October 2003, you should only digitally sign email messages requiring non-repudiation services. Sending encrypted email should be the *exception*, not the *rule*. Only use encryption for:

- Privacy Act information
- For Official Use Only (FOUO) information
- Sensitive But Unclassified (SBU) data
- Health Insurance Portability and Accountability Act information (HIPAA)

To begin operations:

1. Insert your CAC into the card reader.
2. Enter your PIN (when prompted).

Note:

- You have three attempts to enter your PIN correctly.
- On the third incorrect entry, your CAC locks and can no longer be used for PKI services. You must then return to your ID issuance facility to reset your PIN.

Sending Digitally Signed/Encrypted Messages

Access the Outlook Inbox to perform this procedure:

(**Note:** To send an encrypted message, you must first obtain the recipient's public key (see section entitled *Obtaining Public Keys for Encryption*).

1. Open a new message.
2. Click the **To...** button to open your Address Book.
3. Add your recipient(s) from any of the following:
   - Any address list(s) for digitally signed messages
   - The Contacts list for encrypted messages
   - The Global Address List (GAL) for encrypted messages if your organization uses *Publish to GAL* (ask your IMO)
4. Select from the New Mail Message toolbar, the
   - Digital Signature icon for *digitally signed* messages
   - Encryption icon for *encrypted* messages
5. Enter the subject, the message body, and add any attachment(s).
6. Send the message.

Determining a Received Message Type

Note: Clicking an icon in a received message accesses additional security services information related to that icon.

A *digitally signed* message (red seal icon):

Doe, John Signed Message

An *encrypted* message (blue lock icon):

Doe, John Encrypted Message

Messages both digitally signed *and* encrypted initially show only the encryption icon:

Doe, John Encrypted Message

Once opened, both icons appear:

If neither icon appears, the message is neither digitally signed nor encrypted.

Obtaining Public Keys for Encryption

Use either of the following methods to obtain an individual's PKI certificate and its public key.

From a digitally signed message

1. Open a digitally signed message.
2. Right click the email address in the **From:** field, then select **Add to Contacts**.
3. Click the **Certificates** tab to verify that **Certificates (Digital IDs)** lists the new certificate.
4. Click **Save and Close.**

From the DoD PKI directory

1. Access the DoD PKI web site, at either:
   - http://dodpki.c3pki.chamb.disa.mil/
   - http://dodpki.c3pki.den.disa.mil/
2. Click the **Search the Email Directory Server** link and select the **Advanced Search** tab.
3. To search for the individual's last name, change the **where the** box from *full name* to *last name* and enter the last name next to the search button. Click **Search**.
4. Select the desired name by clicking the corresponding **ID** link. The individual's Properties page opens.
5. Click the **Download Certificate** link. This accesses the file download dialog.
6. Select **Save this file to disk** and click **OK** to access the Save As window.
7. Select your desktop as the location to save the certificate.
8. Rename the certificate (the default name provided is *dosearch*.) Use the individual's name plus the .cer extension.
   Convention: [last name][first initial].cer
   Example: John Doe = doej.cer
9. Click **Save** to save the certificate.
10. Click the individual's email address link. Outlook generates a blank new message. If:
    - The email address is underlined, continue
    - The email address is not underlined, click the Check Names icon
11. Right click the email address and select **Add to Contacts**. The Contacts window opens.
12. Click the **Certificates** tab, then the **Import…** button.
13. Select the new certificate from the Desktop.
14. Click **Save and Close**.

For Assistance Contact:

- Your local Information Management Specialist

- PM SET-D Help Desk:
  1-866-SET-DCAC (738-3222)
  Hours of Operation:
  M-F 0600-2100

See the SET-D web site for:

- Help information
- Frequently Asked Questions (FAQs)
- Troubleshooting
- Training information

https://setdweb.setd.army.mil

See Defense Manpower Data Center (DMDC) for ID issuance facility locators:

http://www.dmdc.osd.mil

PEO EIS
PEO Enterprise Information Systems

PM SET-D
SECURE ELECTRONIC TRANSACTIONS DEVICES

Digitally Signed and Encrypted Email Procedures

Product Manager
Secure Electronic Transactions - Devices

PM SET-D